COUNTY OF SAN LUIS OBISPO

Countywide Information Security Program

Administrative Policy

Title:	Information Security Program Remote Access Policy

Effective Date: August 6, 2004
Prepared by: Countywide Information Security Committee
Review Date: August 6, 2006
Approved by: Information Technology Executive Steering Committee
Approval Date: August 6, 2004

1. PURPOSE

To establish policy for allowing only authorized access to the County's computer network from a location that is not physically connected to the County's wide-area-network (WAN), or a departmental local-area-network (LAN).

2. SCOPE

This policy applies to all Users that have been granted remote access ability by their respective departments for the purpose of conducting County business.

3. POLICY

3.1. Overview

3.1.1. All remote access to the County WAN will be accomplished via a secure method, i.e., strong authentication and encryption.

3.1.2. Access from a remote site to a County network that contains data classified as For Official Use Only (FOUO) may require extended identification and authentication procedures. (see the ISP Privacy and Confidentiality Policy for more information)

3.1.3. All Users remotely accessing the County network will exercise due diligence in ensuring that County Computing Assets, and non-County computer systems used for this purpose, are free from viral infections and unauthorized use.

3.1.4. When a (previously) authorized, remote User separates from County employment, is placed on administrative leave, or retires all existing remote access services will be terminated. Interdepartmental transferees will only have their department-specific resources terminated.

3.2. Use and Awareness

3.2.1. See the Countywide Information Security Program Acceptable Use Policy for details regarding authorized use, personal use, security, unacceptable use, and monitoring. Remote access is considered a privilege, and can be revoked at any time without cause by the authorizing department head.

3.2.2. State of California applications such as DMV, MEDS, and CLETS may not be permitted from remote locations due to State security regulations.

3.2.3. Remote sessions that are inactive for more than 30 minutes may be discontinued automatically.

3.2.4. Based on the job function within the County, some departments may find it necessary and beneficial to supply County Computing Assets for use in supporting their applications remotely. If County Computing Assets are to be removed from the County premises, Users must complete an appropriate Authorization for Removal of County Computing Assets form. It must be signed (authorized) and kept on file in their department (sample attached).

3.2.5. Users accessing the County via remote-control applications such as PC Anywhere, VNC, etc., must do so with software issued by their department, and with the full knowledge of their department.

3.2.6. Support will be provided only for County Computing Assets used for remote service. Support will be accomplished by the end User bringing the assigned County Computing Assets to a serviceable County facility. Personal computing assets used for remote access will not be serviced by the County. The County will not be liable for damage to personal computers nor the data stored on them.

3.2.7. Three unsuccessful attempts to sign on to the remote facility due to an incorrect userid or password may result in the temporary revocation of the account. Users must call ITD to have their logon reset.

3.2.8. Application forms and instructions for remote access are available from the Information Technology Department.

4. **DEFINITIONS**

4.1. COMPUTING ASSETS

Information of any kind processed by any means using County information processing systems, networks, software, equipment, materials, or implements which are owned, managed, operated, maintained, or in the custody or proprietorship of the County or private entities. This includes, but is not limited to, Internet, Intranet, and Extranet applications, operating systems, network operating systems, storage media, network accounts, E-mail, file transfer protocol, and documentation.

4.2. USER

Any end User of County Computing Assets including; elected officials, full-time, part-time, and temporary County officers, agents, employees, contractors, consultants, and volunteers or any individual authorized to use County Computing Assets.

5. OTHER AGENCY INVOLVEMENT

The Information Technology Department will work cooperatively with all County departments, outside governmental agencies, and vendors performing information technology work with the County, to ensure safe and secure information systems, as well as to protect the core enterprise architecture.

6. FORMS

ATTACHMENT: Authorization for Removal of County Equipment (SAMPLE)

7. RELATED DOCUMENTS/POLICIES

7.1. Information Security Program:

7.1.1. Acceptable Use Policy

7.1.2. Master Security Policy

7.1.3. Privacy and Confidentiality Policy

8. ENFORCEMENT

Any User of County Computing Assets, found to have willfully violated this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

9. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.1	August 6, 2005	3.1.2 4.2 8.0	Replaced “sensitive or restricted” with FOUO Added “officers, agents” Changed “purposefully” to “willfully”
1.0	August 6, 2004	All	New policy entitled *ISP Remote Access Policy*

ATTACHMENT

(SAMPLE)

TO: All Concerned Parties

FROM: _____ , (department head)

DATE: _____

SUBJECT: **Authorization for Removal of County Computing Assets**

This notice authorizes the following County User to remove the Computing Assets designated below from County premises, for the purpose of conducting County business:

User:	_____	User #:	_____
Item:	_____	Serial No:	_____
Item:	_____	Serial No:	_____
Item:	_____	Serial No:	_____
Item:	_____	Serial No:	_____
Item:	_____	Serial No:	_____

This equipment will be returned to County premises by (circle all that apply):

a. The following date _____ / _____ / _____
b. The need for replacement
c. The User's termination date

User's signature: _____

User's name (printed): _____

Authorizing signature: _____